Discrete Mathematics 66 (1987) 283–288
North-Holland

EXISTENCE OF SELF-REVERSE-DUAL M-SEQUENCES

Zhe-xian WAN and Rong-hua XIONG
Institute of Systems Science, Academic Sinica, Beijing 100080, China

Received 22 October 1985
Revised 3 November 1986

1. Introduction

Let $f(x_0, \ldots, x_{n-1}) = x_0 + f_0(x_1, \ldots, x_{n-1})$ be a nonsingular function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $\mathbb{F}_2$ denotes the Galois field with 2 elements and $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$. A binary sequence $\boldsymbol{a} = (a_0, a_1, a_2, \ldots)$ is called an n-stage feedback shift register sequence with feedback logic f (or generated by f) if $a_{k+n} = f(a_k, a_{k+1}, \ldots, a_{k+n+1})$ for all $k \geq 0$. It is known that any n-stage feedback shift register sequence generated by a nonsingular feedback logic f is periodic. The set of all such sequences generated by f is denoted by $\Omega(f)$, and the state diagram of f is denoted by G_f. If $\boldsymbol{a} \in \Omega(f)$ and the period of $\boldsymbol{a}$ (denoted by $p(\boldsymbol{a})$) is equal to 2^n, then $\boldsymbol{a}$ is called an M-sequence and f an M-logic.

Set

$$\mathrm{Df}(x_0, x_1, \ldots, x_{n-1}) = x_0 + f_0(\bar{x}_1, \ldots, \bar{x}_{n-1}),$$
$$\mathrm{Rf}(x_0, x_1, \ldots, x_{n-1}) = x_0 + f_0(x_{n-1}, \ldots, x_1).$$

Then Df and Rf are called the dual function and the reverse function of f respectively, and RDf(= DRf) is called the reverse-dual function of f. If RDf $= f$, then f is called a self-reverse-dual function, or in short, SRD function.

It is well-known that if f is an n-stage M-logic, then Df, Rf and RDf are all n-stage M-logics, Df $\neq f$, Rf $\neq f$ and RDf $\neq f$ when n is even. But, when n is odd, there may exist n-stage SRD M-logic. For example, $f(x_0, x_1, x_2) = \bar{x}_0 + \bar{x}_1 x_2$ is a 3-stage SRD M-logic. An unsolved problem is whether there exists an n-stage SRD M-logic for all odd $n \geq 1$. In the present paper, an affirmative answer will be given to this problem. The main results are as follows:

Theorem 1. *There exists an n-stage self-reverse-dual M-logic for all odd $n \geq 3$.*

Theorem 2. *The number of all n-stage self-reverse-dual M-logics is a multiple of $2^{\frac{1}{2}(n-1)}$ for all odd $n \geq 3$.*

2. Two lemmas

Let $a=(a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}_2^m$. Set $\mathrm{RD}(a)=(\bar{a}_{m-1}, \ldots, \bar{a}_1, \bar{a}_0)$. Then $\mathrm{RD}: \mathbb{F}_2^m \to \mathbb{F}_2^m$ is a bijection. a is called a self-reverse-dual (or, in short, SRD) element, if $\mathrm{RD}(a)=a$. It is obvious that, for odd m, $\mathrm{RD}(a) \neq a$ for all $a \in \mathbb{F}_2^m$.

From now on, we always assume that n is odd and $\geqslant 3$.

Suppose $f=x_0+f_0(x_1, \ldots, x_{n-1})$, $\boldsymbol{a}=(a_0, a_1, a_2, \ldots) \in \Omega(f)$, and $p(\boldsymbol{a})=p$. Denote the cycle of G_f corresponding to $\boldsymbol{a}$ by $(a_0, a_1, a_2, \ldots, a_{p-1})$ or $(a_i, a_{i+1}, \ldots, a_{i+p-1})$, $i \geqslant 0$, or in brevity by $(\boldsymbol{a})$. Define $\mathrm{RD}(\boldsymbol{a})=(\bar{a}_{p-1}, \ldots, \bar{a}_2, \bar{a}_1, \bar{a}_0)$ and call $\mathrm{RD}(\boldsymbol{a})$ the reversal-dual cycle of $(\boldsymbol{a})$. $(\boldsymbol{a})$ is called an SRD cycle, if $\mathrm{RD}(\boldsymbol{a})=(\boldsymbol{a})$. Obviously, $\mathrm{RD}(\boldsymbol{a})$ is a cycle of $G_{\mathrm{RD}(f)}$, whenever $(\boldsymbol{a})$ is a cycle of G_f. Furthermore, set

$$s_i(\boldsymbol{a})=(a_i, a_{i+1}, \ldots, a_{i+n-1}),$$
$$\tilde{s}_i(\boldsymbol{a})=(a_i, a_{i+1}, \ldots, a_{i+n-1}, a_{i+n}).$$

$s_i(\boldsymbol{a})$ and $\tilde{s}_i(\boldsymbol{a})$ are called an n-state and an $(n+1)$-state of $(\boldsymbol{a})$ respectively. Usually, $s_i(\boldsymbol{a})$ and $\tilde{s}_i(\boldsymbol{a})$ are abbreviated as s_i and $\tilde{s}_i$.

Lemma 1. *Suppose $(\boldsymbol{a})$ is an SRD cycle, then $p(\boldsymbol{a})$ is even and there are only two* SRD$(n+1)$*-states of $(\boldsymbol{a})$.*

Proof. Since $\mathrm{RD}(\boldsymbol{a})=(\boldsymbol{a})$, there exists an integer k, $0 \leqslant k \leqslant p-1$, such that

$$(a_k, a_{k+1}, \ldots, a_{k+p-1})=(\bar{a}_{p-1}, \bar{a}_{p-2}, \ldots, \bar{a}_1, \bar{a}_0). \tag{1}$$

Then for all z, $0 \leqslant z \leqslant p-1$, we have

$$s_{k+z}=\mathrm{RD}(s_{p-z-n}). \tag{2}$$

If one of p and k is odd, then the congruence

$$k+z \equiv p-z-n \pmod{p}$$

has a solution z_0 $(0 \leqslant z_0 \leqslant p-1)$. Thus by (2),

$$s_{k+z_0}=\mathrm{RD}(s_{p-z_0-n})=\mathrm{RD}(s_{k+z_0}).$$

This contradicts the assumption that n is odd. Therefore, both p and k are even. In this case, the congruence

$$k+z \equiv p-z-n-1 \pmod{p}$$

has two and only two solutions z_1 and z_2 satisfying $0 \leqslant z_1, z_2 \leqslant p-1$ and $z_1 \neq z_2$. We have by (1)

$$\tilde{s}_{k+z_1}=\mathrm{RD}(\tilde{s}_{p-z_1-n-1})=\mathrm{RD}(\tilde{s}_{k+z_1}),$$
$$\tilde{s}_{k+z_2}=\mathrm{RD}(\tilde{s}_{p-z_2-n-1})=\mathrm{RD}(\tilde{s}_{k+z_2}).$$

Since $k+z_1 \not\equiv k+z_2 \pmod{p}$, $\tilde{s}_{k+z_1}$ and $\tilde{s}_{k+z_2}$ are two distinct SRD$(n+1)$-states

of $(\boldsymbol{a})$. Now suppose $\tilde{s}_{k+j}$, $0 \leqslant j \leqslant p-1$, is an SRD$(n+1)$-state of $(\boldsymbol{a})$, i.e.,

$$\tilde{s}_{k+j} = \mathrm{RD}(\tilde{s}_{k+j}).$$

But by (1) we have

$$\tilde{s}_{k+j} = \mathrm{RD}(\tilde{s}_{p-j-n-1}).$$

Thus

$$\mathrm{RD}(\tilde{s}_{k+j}) = \mathrm{RD}(\tilde{s}_{p-j-n-1}).$$

Since $\tilde{s}_{k+j}$ occurs at most once in $(\boldsymbol{a})$, we have necessarily $k+j \equiv p-j-n-1 \pmod{p}$. This implies $j = z_1$ or z_2. And the lemma is completely proved. □

Now let $\alpha = (a_1, a_2, \ldots, a_{n-1}) \in \mathbb{F}_2^{n-1}$. We use the notation $X(n-1, \alpha)$ to represent the monomial $x_1^{a_1} x_2^{a_2} \cdots x_{n-1}^{a_{n-1}}$, where

$$x_i^{a_i} = \begin{cases} x_i, & \text{if } a_i = 1, \\ x_i + 1, & \text{if } a_i = 0, \end{cases} \quad (i = 1, 2, \ldots, n-1).$$

Suppose $f(x_0, x_1, \ldots, x_{n-1}) = x_0 + f_0(x_1, \ldots, x_{n-1})$ and let

$$E = \{\alpha \in \mathbb{F}_2^{n-1} \mid f_0(\alpha) = 1\},$$

then

$$f(x_0, x_1, \ldots, x_{n-1}) = x_0 + \sum_{\alpha \in E} X(n-1, \alpha).$$

Define

$$\mathrm{RD}(E) = \{\mathrm{RD}(\alpha) \mid \alpha \in E\}.$$

Then it is easy to see that $\mathrm{RDf} = f$ iff $\mathrm{RD}(E) = E$.

Lemma 2. *Let $f(x_0, x_1, \ldots, x_{n-1}) = x_0 + \sum_{\alpha \in E} X(n-1, \alpha)$ be a self-reverse-dual function, then the number of self-reverse-dual elements in E is equal to the number of self-reverse-dual cycles in G_f.*

Proof. Let $\alpha = (a_1, a_2, \ldots, a_{n-1})$ and set $\tilde{s}_0 = (0, a_1, \ldots, a_{n-1}, 1)$, $\tilde{s}_1 = (1, a_1, \ldots, a_{n-1}, 0)$. Then $\alpha \in E$ iff both $\tilde{s}_0$ and $\tilde{s}_1$ are $(n+1)$-states of some cycles in G_f. And $\mathrm{RD}(\alpha) = \alpha$ iff $\mathrm{RD}(\tilde{s}_i) = \tilde{s}_i$ $(i = 0, 1)$. Thus, if N is the number of SRD elements in E, then $2N$ is the number of SRD$(n+1)$-states of cycles in G_f. By Lemma 1, there are exactly two SRD$(n+1)$-states in every SRD cycle of G_f. On the other hand, there is no SRD$(n+1)$-state on a cycle which is not a SRD one. Hence, the number of SRD cycles in G_f is also N.

3. Proof of Theorem 1

In the first section, we have already mentioned that there is a 3-stage SRD M-logic, i.e., $f(x_0, x_1, x_2) = \bar{x}_0 + \bar{x}_1 x_2$. We shall prove by induction that Theorem 1 holds.

Now let $n \geq 3$ be odd and $f(x_0, x_1, \ldots, x_{n-1}) = x_0 + f_0(x_1, \ldots, x_{n-1})$ be an n-stage SRD M-logic. We shall construct an $(n+2)$-stage SRD M-logic from f as follows. At first, we construct the function

$$g(x_0, x_1, \ldots, x_{n+1}) = x_0 + x_1 + x_2 + f_0(x_1 + x_2 + x_3, \ldots, x_{n-1} + x_n + x_{n+1}) + x_n + x_{n+1}.$$

We have

Lemma 3. *Let f be an n-stage SRD M-logic and $g(x_0, x_1, \ldots, x_{n+1})$ be defined as above. Then* $\mathrm{RDg} = g$ *and G_g consists of two cycles of length 2^n and $3 \cdot 2^n$ respectively.*

Proof. The equality $\mathrm{RDg} = g$ can be verified directly and the second assertion follows from Theorem 3.15 of [2].

Denote the two cycles of G_g by $(\boldsymbol{a})$ and $(\boldsymbol{b})$, where $p(\boldsymbol{a}) = 2^n$, $p(\boldsymbol{b}) = 3 \cdot 2^n$. Since $\mathrm{RDg} = g$ and $p(\boldsymbol{a}) \neq p(\boldsymbol{b})$, we have $\mathrm{RD}(\boldsymbol{a}) = (\boldsymbol{a})$, $\mathrm{RD}(\boldsymbol{b}) = \boldsymbol{b}$. Write $g = x_0 + \sum_{\alpha \in E} X(n+1, \alpha)$, where $E \subset \mathbb{F}_2^{n+1}$, then by Lemma 2, the number of SRD elements in E is 2. Let $\beta \in E$ such that $\mathrm{RD}(\beta) = \beta$. Set $E_1 = E \backslash \{\beta\}$ and $g_1(x_0, x_1, \ldots, x_{n+1}) = g(x_0, x_1, \ldots, x_{n+1}) + X(n+1, \beta)$, then $g_1 = x_0 + \sum_{\alpha \in E_1} X(n+1, \alpha)$ and $\mathrm{RDg}_1 = g_1$. The number of cycles of G_{g_1} is either 1 or 3. We distinguish these two cases

Case 1. G_{g_1} consists of one cycle

In this case, g_1 is an $(n+2)$-stage SRD M-logic.

Case 2. G_{g_1} consists of 3 cycles

Denote the 3 cycles of G_{g_1} by σ_1, σ_2, and σ_3. Since there is only one SRD element in E_1, by Lemma 2, there is only one SRD cycle in G_{g_1}. Since $\mathrm{RDg}_1 = g_1$, we may assume that $\mathrm{RD}(\sigma_1) = \sigma_2$ and $\mathrm{RD}(\sigma_3) = \sigma_3$. Since σ_3 is a cycle of length 2^{n+2}, there exists an $(n+2)$-state $s = (a_0, a_1, \ldots, a_{n+1})$ on σ_3 whose conjugate state $s^* = (\bar{a}_0, a_1, \ldots, a_{n+1})$ does not lie on σ_3. We may assume $s^* = (\bar{a}_0, a_1, \ldots, a_{n+1})$ is on σ_1. Then $\mathrm{RD}(s) = (\bar{a}_{n+1}, \ldots, \bar{a}_1, \bar{a}_0)$ and $\mathrm{RD}(s^*) = (\bar{a}_{n+1}, \ldots, \bar{a}_1, a_0)$ are on cycles σ_3 and σ_2 respectively. Set $\alpha_1 = (a_1, a_2, \ldots, a_{n+1})$, $\alpha_2 = (\bar{a}_{n+1}, \ldots, \bar{a}_2, \bar{a}_1)$ and

$$g_2(x_0, x_1, \ldots, x_{n+1}) = g_1(x_0, x_1, \ldots, x_{n+1}) + X(n+1, \alpha_1) + X(n+1, \alpha_2).$$

Since $\mathrm{RD}(\alpha_1) = \alpha_2$, we have $\mathrm{RDg}_2 = g_2$. Obviously, G_{g_2} is the directed graph obtained by joining σ_1, σ_2 and σ_3 into a single cycle of length 2^{n+2}. Thus $g_2(x_0, x_1, \ldots, x_{n+1})$ is an $(n+2)$-stage SRD M-logic.

Therefore Theorem 1 is proved by mathematical induction. □

4. Proof of Theorem 2

Let $f(x_0, x_1, \ldots, x_{n-1}) = x_0 + \sum_{\alpha \in E} X(n-1, \alpha)$ be an n-stage SRD M-logic. By Lemma 2, there is only one SRD element in E, which will be denoted by α_0. We take an SRD element β from $\mathbb{F}_2^{n-1}$ and let

$$E_\beta = (E \backslash \{\alpha_0\}) \cup \{\beta\},$$

$$f_\beta(x_0, x_1, \ldots, x_{n-1}) = f(x_0, x_1, \ldots, x_{n-1}) + X(n-1, \alpha_0) + X(n-1, \beta),$$

then $f_\beta(x_0, x_1, \ldots, x_{n-1}) = x_0 + \sum_{\alpha \in E_\beta} X(n-1, \alpha)$; since $\mathrm{RD}(E_\beta) = E_\beta$, we have $\mathrm{RD}(f_\beta) = f_\beta$.

We want to prove that f is also a M-logic.

If $\beta = \alpha_0$, then $f_\beta = f$ and the assertion holds. Now, we assume $\beta \neq \alpha_0$, then $\beta \notin E$. Let

$$g(x_0, x_1, \ldots, x_{n-1}) = f(x_0, x_1, \ldots, x_{n-1}) + X(n-1, \alpha_0).$$

then $g = x_0 + \sum_{\alpha \in E_0} X(n-1, \alpha)$, where $E_0 = E \backslash \{\alpha_0\}$, G_g consists of two cycles, which will be denoted by σ_1 and σ_2. Because $\mathrm{RD}(E_0) = E_0$ and E_0 does not contain an SRD element, $\mathrm{RD}g = g$ and G_g does not contain an SRD cycle. Hence we have $\mathrm{RD}(\sigma_1) = \sigma_2$. Write $\beta = (b_1, \ldots, b_{n-1})$ and set $\tilde{s}_0 = (0, b_1, \ldots, b_{n-1}, 0)$, $\tilde{s}_1 = (1, b_1, \ldots, b_{n-1}, 1)$. Since $\beta \notin E_0$, $\tilde{s}_0$ and $\tilde{s}_1$ are $(n+1)$-states of cycles in G_g. Without loss of generality, we can assume $\tilde{s}_0$ is an $(n+1)$-state of σ_1. Then from $\mathrm{RD}(\tilde{s}_0) = \tilde{s}_1$ we deduce that $\tilde{s}_1$ is an $(n+1)$-state of σ_2. This implies that the two conjugate n-states $(0, b_1, \ldots, b_{n-1})$ and $(1, b_1, \ldots, b_{n-1})$ are on the cycles σ_1 and σ_2 respectively. So G_{f_β} consists of one cycle which is obtained by joining σ_1 and σ_2 through β. This shows that f_β is an M-logic.

It is easy to show that there are $2^{\frac{1}{2}(n-1)}$ SRD elements in $\mathbb{F}_2^{n+1}$. By the above discussion we can derive $2^{\frac{1}{2}(n-1)}$ n-stage SRD M-logics from every n-stage SRD M-logic and they can be transformed one into another by using the above method. Therefore the number of n-stage SRD M-logics must be a multiple of $2^{\frac{1}{2}(n-1)}$. This completes the proof of Theorem 2. □

5. An example

We give the following example for illustration.

Let us start with the 3-stage SRD M-logic $f(x_0, x_1, x_2) = \bar{x}_0 + \bar{x}_1 x_2$, which generates the SRD cycle of length $2^3 = 8$,

$$\sigma = (00010111).$$

In σ we have two SRD 4-states (0101) and (1100). This illustrates Lemma 1.

We may write

$$f(x_0, x_1, x_2) = x_0 + f_0(x_1, x_2),$$

where

$$f_0(x_1, x_2) = x_1x_2 + x_1\bar{x}_2 + \bar{x}_1\bar{x}_2.$$

Then

$$E_{f_0} = \{(\alpha_1, \alpha_2) \in \mathbb{F}_2^2 \mid f_0(\alpha_1, \alpha_2) = 1\}$$
$$= \{(11), (10), (00)\}.$$

The number of SRD elements in E_f is 1 and the number of SRD cycles in G_f is also 1. This illustrates Lemma 2.

Put

$$g(x_0, x_1, x_2, x_3, x_4) = x_0 + x_1 + x_2 + f_0(x_1 + x_2 + x_3, x_2 + x_3 + x_4) + x_3 + x_4$$

We may write

$$g(x_0, x_1, x_2, x_3) = x_0 + \sum_{(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in E} x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}x_4^{\alpha_4},$$

where

$$E = \{(1111), (1001), (0111), (0110), (0101), (0011), (0001), (0000)\}.$$

There are exactly two SRD elements in E, i.e., (0101) and (0011). G_g consists of two SRD cycles of length $2^3 = 8$ and $3 \cdot 2^3 = 24$ respectively, i.e.,

$$\sigma_1 = (00110101) \quad \text{and} \quad \sigma_2 = (000001111101110010110001).$$

This illustrates Lemma 3. In this case, both (0101) and (0011) appear as 4-states in σ_1 as well as σ_2. Let $\beta = (0101)$. Set $E_1 = E \backslash \{\beta\}$ and

$$g_1(x_0, x_1, x_2, x_3, x_4) = g(x_0, x_1, x_2, x_3, x_4) + \bar{x}_1x_2\bar{x}_3x_4.$$

Then

$$g_1(x_0, x_1, x_2, x_3, x_4) = x_0 + \sum_{(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in E} x_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}x_4^{\alpha_4}$$

is an SRD function and G_{g_1} consists of an SRD cycle of length $2^5 = 32$. This illustrates the first case of the proof of Theorem 1.

There is only one SRD element in E_1, i.e., (0011). Put

$$g_2(x_0, x_1, x_2, x_3, x_4) = g_1(x_0, x_1, x_2, x_3, x_4) + \bar{x}_1\bar{x}_2x_3x_4.$$

Then

$$g_2(x_0, x_1, x_2, x_3, x_4) = g(x_0, x_1, x_2, x_3, x_4)$$

and we know that G_f consists of two SRD cycles σ_1 and σ_2. There are $2^2 = 4$ SRD 4-states, i.e., (0101), (1010), (0011) and (1100). Any one of them appears both in σ_1 and σ_2. By adding each of $\bar{x}_1x_2\bar{x}_3x_4$, $x_1\bar{x}_2x_3\bar{x}_4$, $\bar{x}_1\bar{x}_2x_3x_4$ and $x_1x_2\bar{x}_3\bar{x}_4$ to $g(x_0, x_1, x_2, x_3, x_4)$ we obtain an SRD M-logic and thus altogether we obtain $2^2 = 4$ SRD M-logics. This illustrates the proof of Theorem 2. □

References

[1] S.W. Golomb, Shift Register Sequences, 2nd ed. (Holden–Day, San Francisco, 1982).

[2] J. Mykkeltveit, M.K. Siu and P. Tong, On the cycle structure of some nonlinear shift register sequences, Inform. and Control 43 (1979) 202–215.